## REMARKS/ARGUMENTS

This Amendment is in response to the Final Office Action dated October 19, 2005. Claims 1-36 are pending in the present application. Claims 1-36 have been rejected. Claims 1-36 remain pending. For the reasons set forth more fully below, Applicants respectfully submit that the claims as presented are allowable. Consequently, reconsideration, allowance, and passage to issue are respectfully requested.

In the event, however, that the Examiner is not persuaded by Applicants' arguments, Applicants respectfully request that the Examiner enter the arguments to clarify issues upon appeal.

### Claim Rejections - 35 U.S.C. §103

The Examiner has stated:

> **Claims 1, 10-12, 24, and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over WO99/67713 (Applicant's Admitted Prior Art) hereinafter, AAPA in view of Lin (USPN: 5,511,184).**
>
> **As per claim 1, AAPA teaches a method for providing a secure data storage system (shown in Figs. 2 and 3), wherein the data storage system is accessed by a processor (CPU 2, in Figs. 2-3), the method comprising the steps of: (a) creating a plurality of logical partitions (16, 18 and 20 in Fig. 5) and (c) hiding at least one partition from the processor (e.g. see the abstract). AAPA does not specifically disclose about creating a backup partition and backing up the logical partitions to the backup partition. However, this feature of step (b), i.e. creating a backup partition and backing up the logical partitions to the backup partition so the data can be retrieved from the backup partition in case of the data stored on one or more logical partitions get corrupted or lost, is well-known and notorious old in the art. The Examiner herein taking Official Notice on this subject matter.**
>
> **The further limitation of step (d), i.e. "automatically blocking low-level physical drive write commands, thereby preventing a virus from using such a command to destroy data on the logical and backup partitions" is not taught by AAPA. However, Lin discloses "prevention of a virus attack at boot time is achieved by write-protecting the storage devices of the system", i.e. blocking low-level physical drive write commands (e.g. see the abstract of AAPA). Accordingly, it would have been obvious to one of ordinary skill in the art at the time of the current invention was made to implement the teachings of Lin in AAPA's method so the data is prevented from a virus program that can destroy/corrupt the data stored on the storage devices. Therefore, it is advantageous...**

**Claims 2-9, 13-23, 25-32 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Lin, further in view of Yuan et al. (USPN: 6,526,477) herein after, Yuan...**

**Remarks**

**As to remark, with respect to claims 1, 14 and 24, Applicant asserted that AAPA does not teach or suggest "hiding the backup partition from the processor," as recited in independent claims 1, 14 and 24. Applicant asserted that the Examiner has referred to the Abstract of the specification as teaching this feature. However, the Abstract of the specification is not AAPA, but it is instead the abstract of the present invention.**

**Examiner respectfully traverses Applicant's remark for the following reasons:**

**The AAPA, i.e. WO99/67713, clearly teaches the limitation of hiding the backup partition from the processor in the abstract of the AAPA not the abstract of the present application. The abstract of the AAPA clearly states as, "The VDS controller (12) partitions the memory system (6) into multiple virtual data storage devices (16, 18), and then restricts the computer system from communicating with certain of these virtual data storage devices (16, 18). The VDS controller (12) thus selectively isolates at least one of the virtual data storage devices (16) from communicating with the computer system, in order to prevent corruption of information stored in at least one virtual data storage device (16)." (e.g. see the Abstract of AAPA). In other words, AAPA does teach the claimed limitation of hiding the backup partition (i.e. at least one of the virtual data storage devices, 16) from the processor (i.e. the computer system).**

Applicants respectfully disagree with the Examiner's rejections. The present invention provides a secure data storage system, where the data storage system is accessed by a processor. In accordance with the present invention, the method includes creating a plurality of logical partitions and creating a backup partition and backing up the logical partitions to the backup partition. The method further includes hiding the backup partition from the processor, and automatically blocking low-level physical drive write commands, thereby preventing a virus from using such a command to destroy data on the logical and backup partitions. Applicants' admitted prior art (AAPA) in view of Yin does not teach or suggest these features, as discussed below.

AAPA discloses a virtual disk storage (VDS) system for providing multiple virtual data storage devices for use in a computer system that contains a central processing unit (CPU). The VDS system includes a memory system for storing information and a VDS controller that is in

communication with the memory system and the CPU. The VDS controller partitions the memory system into multiple virtual data storage devices, and then restricts the computer system from communicating with certain of these virtual data storage devices. The VDS controller thus selectively isolates at least one of the virtual data storage devices from communicating with the other computer system, in order to prevent corruption of information stored in at least one virtual data storage device. (Abstract.)

The Examiner has recognized that AAPA does not disclose "creating a backup partition and backing up the logical partitions to the backup partition," as recited in claims 1, 14, and 24. The Examiner has asserted, however, that the step of "creating a backup partition and backing up the logical partitions to the backup partition so that data can be retrieved from the backup partition in case of the data stored on the one or more of the logical partitions get corrupted or lost" is well-known and the Examiner has taken Official Notice on this subject matter. Applicants respectfully disagrees.

While Applicants recognize that the Examiner is entitled to support an obviousness rejection based on common knowledge in the art, Applicants respectfully submit that the Examiner can only take official notice of facts outside the record which are capable of instant and unquestionable demonstration of being "well-known" in the art. In re Ahlert, 424 F.2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970). In the present case, Applicant submits that one of skill in the art would not have created a backup partition and backed up logical partitions to the backup partition as specifically discussed in the background section of Applicant's specification at page 3, lines 3-13.

Applicant respectfully requests the Examiner to cite a reference that provides a teaching or suggestion to create a backup partition and backup logical partitions to the backup partition. Or if the Examiner is basing the rejection on personal facts within the knowledge of the Examiner, Applicant respectfully requests that the Examiner provide an affidavit to support those facts. See MPEP 2144.03; 37 CFR 1.104 (d)(2).

A secondary reference stands or falls with the primary reference. Because AAPA fails to teach or suggest "creating a backup partition and backing up the logical partitions to the backup partition," a combination of AAPA and Lin also fails to teach or suggest the claimed invention. Accordingly, independent claims 1, 14, and 24 allowable over AAPA in view of Lin.

Furthermore, Applicants agree with the Examiner that AAPA does not teach "automatically blocking low-level physical drive write commands, thereby preventing a virus from using such a command to destroy data on the logical and backup partitions," as recited in independent claims 1, 14, and 24. The Examiner has relied upon Lin, referring to the abstract, to cure the defects of AAPA with regard to this feature. Lin discloses a method and apparatus for protecting a computer system from computer viruses. Detection and prevention of a virus attack at boot time is achieved by write-protecting the storage devices of the system before the booting process and by detecting the presence of virus by checking integrity of the interrupt vectors of the system. Similar checks may be run on the system modules, device drivers, and application programs, using, for example, a checksum to insure that no further viruses are present in those programs. (Abstract.)

However, the abstract of Lin merely mentions "write-protecting the storage devices of the system before the booting process." Lin fails to specifically describe "automatically blocking **low-level physical drive** write commands" as in the present invention.

Therefore, AAPA in view of Lin does not teach or suggest the combination of steps as recited in independent claims 1, 14, and 24, and these claims are allowable over AAPA in view of Lin.

Dependent claims

Dependent claims 2-13, 15-23, and 25-36 depend from independent claims 1, 14, and 24, respectively. Accordingly, the above-articulated arguments related to independent claims 1, 14, and 24 apply with equal force to claims 2-13, 15-23, and 25-36, which are thus allowable over the cited references for at least the same reasons as claims 1, 14, and 24.

Conclusion

In view of the foregoing, Applicants submit that claims 1-36 are patentable over the cited references. Applicants, therefore, respectfully request reconsideration and allowance of the claims as now presented.

Applicants' attorney believes that this application is in condition for allowance. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

December 19, 2005
Date

Joseph A. Sawyer, Jr.
Attorney for Applicant(s)
Reg. No. 30,801
(650) 493-4540